PathResolve

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3344 bytes

Attack Category	• Malicious Input
Vulnerability Category	• Buffer Overflow • Unconditional
Software Context	• File Path Management
Location	• shlobj.h
Description	The destination string buffer for PathResolve() must be long enough to hold the fully qualified path. The PathResolve() routine converts a relative path to a fully qualified pathname. It modifies the path parameter in place.
APIs	**Function Name** | **Comments** PathResolve |
Method of Attack	The pszPath variable is modified in place to contain the fully qualified path. If the attacker provides a relative path to a very long path name, this could overflow the buffer. Furthermore, if the string buffer is declared exactly the size of the input string, a buffer overflow is almost guaranteed to occur.
Exception Criteria	
Solutions	**Solution Applicability** | **Solution Description** | **Solution Efficacy** Whenever PathResolve() is called. | The first parameter, pszPath, must be at least MAX_PATH characters in length. | Effective
Signature Details	BOOL PathResolve(LPWSTR pszPath, LPCWSTR *dirs, UINT fFlags);

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

Examples of Incorrect Code	`WCHAR path[] = L"MyFile.dat"; // Buffer is too small`
	`LPWSTR pszPath = path;`
	`LPCWSTR dirs[] = { NULL };`
	`if (!PathResolve(pszPath, dirs, PRF_VERIFYEXISTS)`
	`{ handleError(); }`

Examples of Corrected Code	`WCHAR path[MAX_PATH] = L"MyFile.dat"; // Buffer is correctly sized`
	`LPWSTR pszPath = path;`
	`LPCWSTR dirs[] = { NULL };`
	`if (!PathResolve(pszPath, dirs, PRF_VERIFYEXISTS)`
	`{ handleError(); }`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/pathresolve.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com